



## ***Guidelines for Completing the Privacy Breach Reporting Form***

Section 64 (4) of *ATIPPA*, 2015 states:

**Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.**

The attached Privacy Breach Reporting Form is to be completed and submitted to the Office of the Information and Privacy Commissioner (OIPC) and ATIPP Office immediately once you become aware of a privacy breach within your public body.

For more information on completing this form, please e-mail the OIPC at [breachreport@oipc.nl.ca](mailto:breachreport@oipc.nl.ca) or call 1-877-729-6309.

For more general information on privacy breaches please refer to the [Privacy Breach Protocol](#) document available on the ATIPP Office website, e-mail: [ATIPPOffice@gov.nl.ca](mailto:ATIPPOffice@gov.nl.ca) or call 1-877-895-8891.

**Information contained in this form will be recorded for breach management purposes, including but not limited to statistical, educational, and investigative purposes. Should the Commissioner decide to initiate a privacy investigation, the public body will be notified.**

**Do not include information in this form that can identify the individual(s)  
whose information has been breached.**

When describing the breach be as specific as possible regarding dates the breach occurred and was discovered. Provide detailed information regarding the nature of the breach including whether the breach occurred as a result of a misdirected e-mail or fax, an error in mail out, due to human error or as a result of a technical malfunction or other cause. Provide additional information in the reporting e-mail or on a separate page if space on the form is not sufficient to include the necessary details.

Note the geographical location of the breach. Many public bodies have offices across the Province; the OIPC is seeking information pertaining to the geographical location of the breach.

Provide precise details as to the number of affected individuals. Where the number is yet unknown provide your best estimate of the number of affected individuals.

Identify the type of personal information contained in the breach. The list provided is not meant to be exhaustive, but merely representative of the more common types of personal information involved in a breach.

When describing the types of safeguards your public body has in place, check only the safeguards relevant to the breach at hand. For example: password protected computers are not relevant to a breach resulting from a letter not being sealed, but would be relevant to a laptop that was stolen.

It may be difficult to predict the nature of the potential harm; carefully analyze and use your experience to identify potential adverse effects of the breach.

Please advise if you have contacted the affected individual. If you have not done so, we need to know why you have chosen not to notify them. If you are still assessing the situation to determine if notification is necessary, please explain.